

# DETERMINING CYCLICITY OF FINITE MODULES

H. W. LENSTRA, JR. AND A. SILVERBERG

ABSTRACT. We present a deterministic polynomial-time algorithm that determines whether a finite module over a finite commutative ring is cyclic, and if it is, outputs a generator.

## 1. INTRODUCTION

If  $R$  is a commutative ring, then an  $R$ -module  $M$  is cyclic if there exists  $y \in M$  such that  $M = Ry$ .

**Theorem 1.1.** *There is a deterministic polynomial-time algorithm that, given a finite commutative ring  $R$  and a finite  $R$ -module  $M$ , decides whether there exists  $y \in M$  such that  $M = Ry$ , and if there is, finds such a  $y$ .*

We present the algorithm in Algorithm 4.1 below. The inputs are given as follows. The ring  $R$  is given as an abelian group by generators and relations, along with all the products of pairs of generators. The finite  $R$ -module  $M$  is given as an abelian group, and for all generators of the abelian groups  $R$  and all generators of the abelian group  $M$  we are given the module products in  $M$ .

Our algorithm depends on  $R$  being an Artin ring, and should generalize to finitely generated modules over any commutative Artin ring that is computationally accessible.

Theorem 1.1 is one of the ingredients of our work [4, 5] on lattices with symmetry, and a sketch of the proof is contained in [4]. Previously published algorithms of the same nature appear to restrict to rings that are algebras over fields. Subsequently to [4], I. Ciocănea-Teodorescu [2], using different and more elaborate techniques, greatly generalized our result, dropping the commutativity assumption on the finite ring  $R$  and finding, for any given finite  $R$ -module  $M$ , a set of generators for  $M$  of smallest possible size.

See Chapter 8 of [1] for commutative algebra background. For the purposes of this paper, commutative rings have an identity element 1, which may be 0.

## 2. LEMMAS ON COMMUTATIVE RINGS

If  $R$  is a commutative ring and  $\mathfrak{a}$  is an ideal in  $R$ , let  $\text{Ann}_R \mathfrak{a}$  denote the annihilator of  $\mathfrak{a}$  in  $R$ . We will use that every finite commutative ring is an Artin ring,

---

*Key words and phrases.* algebraic algorithms, finite rings, cyclic modules.

This material is based on research sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750-13-2-0054 and by the Alfred P. Sloan Foundation. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

that every Artin ring is isomorphic to a finite direct product of local Artin rings, and that the maximal ideal in a local Artin ring is always nilpotent.

**Lemma 2.1.** *If  $A$  is a local Artin ring,  $\mathfrak{a}$  is an ideal in  $A$ , and  $\mathfrak{a}^2 = \mathfrak{a}$ , then  $\mathfrak{a}$  is 0 or  $A$ .*

*Proof.* If  $\mathfrak{a}$  contains a unit, then  $\mathfrak{a} = A$ . Otherwise,  $\mathfrak{a}$  is contained in the maximal ideal  $\mathfrak{m}$ , which is nilpotent. Thus there is an  $r \in \mathbb{Z}_{>0}$  such that  $\mathfrak{m}^r = 0$ . Now  $\mathfrak{a} = \mathfrak{a}^2 = \dots = \mathfrak{a}^r \subset \mathfrak{m}^r = 0$ .  $\square$

**Lemma 2.2.** *Suppose that  $A$  is a finite commutative ring,  $\mathfrak{a}$  is an ideal in  $A$ ,  $\mathfrak{b} = \text{Ann}_A \mathfrak{a}$ , and  $\mathfrak{a} \cap \mathfrak{b} = 0$ . Then:*

- (i)  $\mathfrak{a}^2 = \mathfrak{a}$ ;
- (ii) *there is an idempotent  $e \in A$  such that  $\mathfrak{a} = eA$ ,  $\mathfrak{b} = (1 - e)A$ , and  $A = (1 - e)A \oplus eA = \mathfrak{b} \oplus \mathfrak{a}$ ;*
- (iii) *if  $\mathfrak{b} = 0$  then  $\mathfrak{a} = A$ .*

*Proof.* Write  $A$  as a finite direct product of local Artin rings  $A_1 \times \dots \times A_s$ . Then  $\mathfrak{a}$  is a direct product  $\mathfrak{a}_1 \times \dots \times \mathfrak{a}_s$  of ideals  $\mathfrak{a}_i \subset A_i$ . Assume  $\mathfrak{a}^2 \neq \mathfrak{a}$ . Then there is an  $i$  such that  $\mathfrak{a}_i^2 \neq \mathfrak{a}_i$ . Let  $\mathfrak{b}_i = \text{Ann}_{A_i} \mathfrak{a}_i$ . Since  $\mathfrak{a} \cap \mathfrak{b} = 0$ , it follows that  $\mathfrak{a}_i \cap \mathfrak{b}_i = 0$ . Since  $A_i$  is a local ring,  $\mathfrak{a}_i$  is contained in the maximal ideal of  $A_i$ , so  $\mathfrak{a}_i$  is nilpotent. Let  $r$  denote the smallest positive integer such that  $\mathfrak{a}_i^r = 0$ . Since  $\mathfrak{a}_i \neq 0$  we have  $r \geq 2$ . Then  $\mathfrak{a}_i^{r-1}$  is contained in  $\mathfrak{a}_i$  and kills  $\mathfrak{a}_i$ , so  $0 \neq \mathfrak{a}_i^{r-1} \subset \mathfrak{a}_i \cap \mathfrak{b}_i = 0$ , a contradiction. This gives (i).

Since  $A$  is a finite product of local Artin rings,  $\mathfrak{a}$  is generated by an idempotent  $e$ , by Lemma 2.1. Then  $\mathfrak{b} = (1 - e)A$  and  $A = (1 - e)A \oplus eA = \mathfrak{b} \oplus \mathfrak{a}$ . This gives (ii) and (iii).  $\square$

### 3. PREPARATORY LEMMAS

If  $R$  is a commutative ring, then a commutative  $R$ -algebra is a commutative ring  $A$  equipped with a ring homomorphism from  $R$  to  $A$ . Whenever  $A$  is an  $R$ -algebra, we let  $M_A$  denote the  $A$ -module  $A \otimes_R M$ .

From now on, suppose  $R$  is finite commutative ring and  $M$  is a finite  $R$ -module. Let  $\mathcal{S}$  denote the set of quadruples  $(A, B, y, N)$  such that:

- (i)  $A$  and  $B$  are finite commutative  $R$ -algebras for which the natural map  $f : R \rightarrow A \times B$  is surjective and has nilpotent kernel,
- (ii)  $y \in M$  is such that the map  $B \rightarrow M_B = B \otimes_R M$  defined by  $b \mapsto b \otimes y$  is an isomorphism and such that  $1 \otimes y = 0$  in  $M_A$ ,
- (iii) and  $N$  is a submodule of  $M$  such that the natural map  $N \rightarrow M_A$  defined by  $z \mapsto 1 \otimes z$  is onto and such that the natural map  $N \rightarrow M_B$  is the zero map.

In Algorithm 4.1 below, initially we take  $(A, B, y, N) = (R, 0, 0, M)$ . Clearly,  $(R, 0, 0, M) \in \mathcal{S}$ . Throughout that algorithm, we always have  $(A, B, y, N) \in \mathcal{S}$ . While  $A$  and  $B$  occur in the proof of correctness of Algorithm 4.1, the  $R$ -algebra  $B$  does not actually occur in the algorithm itself.

**Lemma 3.1.** *If  $(A, B, y, N) \in \mathcal{S}$  and  $M_A = 0$ , then  $M = Ry$ .*

*Proof.* Let  $J$  denote the kernel of  $f : R \rightarrow A \times B$ , and let  $I_A$  (resp.,  $I_B$ ) denote the kernel of the composition of  $f$  with projection from  $A \times B$  onto  $A$  (resp.,  $B$ ). Since  $J$  is nilpotent we have  $J^r = 0$  for some  $r \in \mathbb{Z}_{>0}$ . Since  $0 = M_A =$

$A \otimes_R M = (R/I_A) \otimes_R M \cong M/I_A M$  it follows that  $I_A M = M$ . Since  $JM \subseteq I_B M = I_B I_A M \subseteq (I_B \cap I_A)M = JM$ , it follows that  $JM = I_B M$ . Letting  $y' = (y \bmod I_B M) \in M/I_B M$ , then  $M_B \cong M/I_B M = By'$ . Thus,

$$\begin{aligned} M &= Ry + I_B M = Ry + JM = Ry + J(Ry + JM) \\ &= Ry + J^2 M = \dots = Ry + J^r M = Ry. \end{aligned}$$

□

**Lemma 3.2.** *Suppose  $(A, B, y, N) \in \mathcal{S}$  and  $M_A \neq 0$ . Then there exists  $x \in N$  such that  $1 \otimes x \neq 0$  in  $M_A$ . Choosing  $x$  and letting  $\mathbf{a} = \text{Ann}_A(1 \otimes x)$  and  $\mathbf{b} = \text{Ann}_A \mathbf{a}$ , we have:*

- (i)  $(A/(\mathbf{a} \cap \mathbf{b}), B, y, N) \in \mathcal{S}$ ;
- (ii) If  $\mathbf{a} \cap \mathbf{b} = 0$  and  $(A/\mathbf{a}) \otimes x = M_{A/\mathbf{a}}$ , then  $(A/\mathbf{b}, (A/\mathbf{a}) \times B, x + y, \mathbf{a}N) \in \mathcal{S}$ , where  $\mathbf{a}N$  denotes  $f^{-1}(\mathbf{a} \times B)N$ .
- (iii) If  $\mathbf{a} \cap \mathbf{b} = 0$  and  $(A/\mathbf{a}) \otimes x \neq M_{A/\mathbf{a}}$ , then  $M$  is not cyclic.

*Proof.* Since the map  $N \rightarrow M_A, z \mapsto 1 \otimes z$  is onto, as long as  $M_A \neq 0$  there exists  $x \in N$  such that  $1 \otimes x \neq 0$  in  $M_A$ .

Since  $\mathbf{a}\mathbf{b} = 0$ , we have  $(\mathbf{a} \cap \mathbf{b})^2 = 0$ , so  $\mathbf{a} \cap \mathbf{b}$  is a nilpotent ideal in  $A$ . It follows that  $(A/(\mathbf{a} \cap \mathbf{b}), B, y, N) \in \mathcal{S}$ , giving (i).

From now on, suppose that  $\mathbf{a} \cap \mathbf{b} = 0$ . By Lemma 2.2, there is an idempotent  $e \in A$  such that  $\mathbf{a} = eA$ ,  $\mathbf{b} = (1 - e)A$ , and  $A = (1 - e)A \oplus eA = \mathbf{b} \oplus \mathbf{a}$ . It follows that  $A \xrightarrow{\sim} A/\mathbf{a} \times A/\mathbf{b}$ , so  $M_A \xrightarrow{\sim} M_{A/\mathbf{a}} \times M_{A/\mathbf{b}}$ . If  $(x', x'')$  is the image of  $1 \otimes x$  under the latter map, then  $x'' = 0$  (we have  $\mathbf{b}x'' = 0$  since  $x'' \in (A/\mathbf{b}) \otimes_R M$ , and  $\mathbf{a}x'' = 0$  since  $\mathbf{a}(1 \otimes x) = 0$ ; thus  $Ax'' = (\mathbf{a} + \mathbf{b})x'' = 0$ , so  $x'' = 0$ ). The map  $i_{\mathbf{a}} : A/\mathbf{a} \rightarrow M_{A/\mathbf{a}}$  defined by  $i_{\mathbf{a}}(t) = tx' = t \otimes x$  is injective since  $\text{Ann}_{A/\mathbf{a}} x' = 0$ .

First suppose  $(A/\mathbf{a}) \otimes x = M_{A/\mathbf{a}}$ . Then the injective map  $i_{\mathbf{a}}$  is an isomorphism. Since  $0 = x'' = 1_{A/\mathbf{b}} \otimes x$ , we have  $1 \otimes (x + y) = 0$  in  $M_{A/\mathbf{b}}$ . It is now easy to check that  $(A/\mathbf{b}, (A/\mathbf{a}) \times B, x + y, \mathbf{a}N) \in \mathcal{S}$ , giving (ii). Note that  $\mathbf{b} \neq 0$  (if  $\mathbf{b} = 0$ , then  $\mathbf{a} = A$  by Lemma 2.2, contradicting that  $1 \otimes x \neq 0$  in  $M_A$ ).

Now suppose that  $(A/\mathbf{a}) \otimes x \neq M_{A/\mathbf{a}}$ . By way of contradiction, suppose  $M$  is a cyclic  $R$ -module. Then  $M_{A/\mathbf{a}}$  is a cyclic  $A/\mathbf{a}$ -module. Since the domain and codomain of  $i_{\mathbf{a}} : A/\mathbf{a} \hookrightarrow M_{A/\mathbf{a}}$  are both finite, it now follows that  $i_{\mathbf{a}}$  is surjective, so  $(A/\mathbf{a}) \otimes x = M_{A/\mathbf{a}}$ . This contradiction gives (iii). □

The intuition behind Algorithm 4.1 is that throughout the algorithm,  $y$  generates the “non- $A$  part” of  $M$ , and the goal is to shrink the “ $A$ -part” of  $M$ , namely  $N$ .

#### 4. MAIN ALGORITHM

**Algorithm 4.1.** Input a finite commutative ring  $R$  and a finite  $R$ -module  $M$ . Decide whether there exists  $y \in M$  such that  $M = Ry$ , and if there is, find such a  $y$ .

- (i) Initially, take  $A = R$ ,  $y = 0$ , and  $N = M$ .
- (ii) If  $M_A = 0$ , stop and output “yes” with generator  $y$ .
- (iii) Otherwise, pick  $x \in N$  such that  $1 \otimes x \neq 0$  in  $M_A$ , and compute  $\mathbf{a} = \text{Ann}_A(1 \otimes x)$ ,  $\mathbf{b} = \text{Ann}_A \mathbf{a}$ , and  $\mathbf{a} \cap \mathbf{b}$ .
- (iv) If  $\mathbf{a} \cap \mathbf{b} \neq 0$ , replace  $A$  by  $A/(\mathbf{a} \cap \mathbf{b})$  and go back to step (ii).

- (v) If  $\mathbf{a} \cap \mathbf{b} = 0$ , then if  $(A/\mathbf{a}) \otimes x \neq M_{A/\mathbf{a}}$  terminate with “no”, and if  $(A/\mathbf{a}) \otimes x = M_{A/\mathbf{a}}$  replace  $A$ ,  $y$ , and  $N$  by  $A/\mathbf{b}$ ,  $x+y$ , and  $\mathbf{a}N$ , respectively, and go back to step (ii).

**Proposition 4.2.** *Algorithm 4.1 runs in polynomial time, and on input a finite commutative ring  $R$  and a finite  $R$ -module  $M$ , decides whether there exists  $y \in M$  such that  $M = Ry$ , and if there is, finds such a  $y$ .*

*Proof.* Since  $A$  is a finite ring, if the algorithm does not stop with “no” then eventually  $A = 0$  and  $M_A = 0$ . Step (ii) of the algorithm is justified by Lemma 3.1, while steps (iii), (iv), and (v) are justified by Lemma 3.2.

The computations of annihilators and of the decompositions  $A \xrightarrow{\sim} A/\mathbf{a} \times A/\mathbf{b}$  can be done in polynomial time using linear algebra (see §14 of [3]); in particular,  $\mathbf{a}$  is the kernel of the map  $A \rightarrow M_A$  defined by  $t \mapsto t(1 \otimes x)$ . For any  $B$ , compute  $M_B$  by computing  $M/I_B M$  (and analogously for  $M_A$ ). Each new  $A$  is at most half the size of the  $A$  it replaces. This implies that the number of steps is at most linear in the length of the input.  $\square$

## REFERENCES

- [1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, MA, 1969.
- [2] I. Ciocănea-Teodorescu, *The module isomorphism problem for finite rings and related results*, Abstract of a talk at the CAAFRTA session of the 20th Conference on Applications of Computer Algebra, July 10, 2014, <http://www.singacom.uva.es/~edgar/caafrrta2014/files/Ciocanea.pdf>.
- [3] H. W. Lenstra, Jr., *Lattices*, in *Algorithmic number theory: lattices, number fields, curves and cryptography*, Math. Sci. Res. Inst. Publ. **44**, Cambridge Univ. Press, Cambridge, 2008, 127–181.
- [4] H. W. Lenstra, Jr. and A. Silverberg, *Revisiting the Gentry-Szydło Algorithm*, in *Advances in Cryptology—CRYPTO 2014*, Lect. Notes in Comp. Sci. **8616**, Springer, Berlin, 2014, 280–296.
- [5] H. W. Lenstra, Jr. and A. Silverberg, *Lattices with symmetry*, submitted.

MATHEMATISCH INSTITUUT, UNIVERSITEIT LEIDEN, POSTBUS 9512, 2300 RA LEIDEN, THE NETHERLANDS

*E-mail address:* hwl@math.leidenuniv.nl

DEPARTMENT OF MATHEMATICS, ROWLAND HALL, UNIVERSITY OF CALIFORNIA, IRVINE, CA 92697, USA

*E-mail address:* asilverb@uci.edu